UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,690	09/12/2003	David D. Brandt	03AB014B/ALBRP303USB	7383

7590 01/09/2008

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
KIM, TAE K	
ART UNIT	PAPER NUMBER
2153	
MAIL DATE	DELIVERY MODE
01/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

40

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/661,690	BRANDT ET AL.	
	Examiner	**Art Unit**	
	Tae K. Kim	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 21 December 2007.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-31 is/are pending in the application.

4a) Of the above claim(s) 6 and 7 is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-5 and 8-31 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 12 September 2003 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 12/21/07.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This is in response to the Applicant's response filed on December 21, 2007. Claims 6 and 7 have been cancelled by the Applicant. Claims 1 – 5 and 8 – 31, where Claims 1, 17, 24, 25, and 28 are in independent form, are presented for examination.

Claim Objections

With regards to the amendments to Claim 1 to clarify the claim language, the Examiner has withdrawn the objection to Claim 1.

With regards to the objection to Claim 7, the Applicant has cancelled the claim. Examiner has withdrawn the objection to Claim 7.

With regards to the objection to Claim 17, the Examiner has withdrawn the objection as it was improper for an independent claim.

With regards to the objections to Claims 2, 18, 19, and 29, the Applicant has not made the suggested changes. The Examiner maintains the objections to Claims 2, 18, 19, and 29, regarding grammar and spelling errors.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1 – 5 and 8 – 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Amended Claim 1, which states "the factory protocol lowers encryption protocol standards for real time performance," is not supported within the specification. Adapting the factory protocol to lower encryption protocol standards for real time performance is supported within the specification (*See Pg. 8, Line 14 - Pg. 9, Line 28*).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 – 5, 8 – 16, and 24 – 27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The system disclosed in Claims 1, 24 and 25, as amended, are software per se. As stated in the specification (Pg. 8, Lines 4-7), the term "protocol," "component" and the like can be referring to software alone. There is nothing within the claim language that states the use of hardware within the system. Claims 2 – 5 and 8 – 16 are dependent on Claim 1 and the claims do not remedy the deficiency found in Claim 1. Likewise, Claims 26 and 27 are dependent on Claim 25 and the claims do not remedy the deficiency found in Claim 25.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 - 5 and 8 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. application 2002/0163920 A1 filed by Walker et al. (hereinafter referenced as "Walker") in view of U.S. patent 5,604,914, invented by Akiyoshi Kabe (hereinafter referenced as "Kabe"), and in further view of U.S. Patent 6,842,850 B1, invented by Dennis K. Branstad et al. (hereinafter referenced as "Branstad").

1. Regarding Claims 1 - 3, 8, 17, 20, 21, and 24, Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). The data can also be sent as an open-ended message (pg. 6, paragraph 0053). Walker, however, does not specifically use this method and apparatus within the automated factory setting. Nor does Walker disclose that the security system comprises of employing weak encryption protocols for real-time performance and strong security protocols for added security.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). Kabe also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). It would be obvious to one skilled in the art to combine the teachings within Kabe and Walker to increase routing efficiency and security within an automated factory setting. Once the factory network became accessible remotely, it also heeded to be protected by the network security measures used outside the automated factory setting. Kabe, however, does not specifically disclose that the security system comprises of employing weak encryption protocols for real-time performance and strong security protocols for added security.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds (Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61). Branstad further discloses that the levels of security at one level may make network connections too slow to process real-time high-speed video (Col. 1, Lines 26-34) and that selectively authenticating data, as described above, is a method to remedy that issue. It would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Branstad with Walker and Kabe to modify the level of security authentication needed for the data packets being transmitted within the network. This would allow more urgent communications to be processed faster and decrease the time needed to authenticate data related to real-time media, such as streaming video and audio, which are intermittent if authentication mechanisms are too strong.

2. Regarding Claims 4 and 5, Walker, in view of Kabe, in further view of Branstad, discloses all the limitations of Claim 1. Kabe further discloses several types of devices

that can be connected to an automated factory network, such as a computer, controller, robot, etc. (col. 1, lines 27- 32). Furthermore, Walker establishes a communication channel within a private, VPN, and information network (pg. 4, paragraph 0035) while Kabe discloses a factory network (col. 1, lines 25-30). Kabe, Walker, or Branstad, do not specifically disclose the communication assets being comprised of an I/O device, a Human Interface Machine, a network device, an I/O module, a sensor actuator, a network sensor, and a network device or that the communication channel can be established in a public, wireless, control, or instrumentation network.

It is commonly known to one of ordinary skill in the art at the application date that many of the devices connected to the factory network will be or be a combination of an I/O device, a Human Interface Machine, an I/O module, a sensor actuator, a network sensor, and a network device. Additionally, It is commonly known that a system that uses a (virtual private network) VPN tunnel (can also use a public network and a wireless network to establish a communication channel. It is also known that a factory network comprises of controllers and various instruments. It is obvious to one skilled in the art that these various devices would be included in a factory automation environment. For each component to communicate with another in a network setting, they need to be connected to a network device and sensor, comprise of an I/O device or I/O module, and be controlled by a Human Interface Machine. Furthermore, any automated robotics comprises of a sensor actuator to control its movements. A VPN tunnel provides additional security within a public network that uses, for example, IP addresses to route destinations. A factory that includes robotics for factory automation uses those instruments within a control environment.

3. Regarding Claims 9 – 16, 18, 19, , Walker, in view of Kabe, in further view of Branstad, discloses all the limitations of Claim 1 above. However, they do not specifically disclose that the factory protocol includes at least a time component, message integrity component, digital signature, sequence field to mitigate replaying old packets, pseudo random sequence, encryption field, or dynamic security adjustment field. There is also no specific disclosure of the factory protocol adapting to a Control and Information Protocol (CIP) or an object model that protects configuration of and transport of data between intelligent devices or associating with a protocol supporting at least one of a Temporal Key Interchange Protocol (TKIP) and a wireless protocol. Walker or Kabe do not specifically disclose of components providing source validation for identification, perform message digest checking for integrity checking, perform check sum tests, provide integrity mechanisms, provide encryption mechanisms, and provide refresh security protocols. Nor do they specifically reference establishing a network trust by an identification, an authentication, an authorization, or a ciphersuite negotiation. Neither is the specific employment of an Elliptical function, an Aziz/Diffie Protocol, a Kerberos protocol, a Beller-Yacobi Protocol, an Extensible authentication protocol (EAP), an MSR+DH protocol, a Future Public Land Mobile Telecommunication Systems Wireless Protocols (FPLMTS), a Beller- Chang-Yacobi Protocol, a Diffie-Hellman Key Exchange, a Parks Protocol, an ASPECT Protocol, a TMN Protocol, RADIUS, Groupe Special Mobile (GSM) protocol, a Cellular Digital Packet Data (CDPD) protocol, a Control and Information Protocol (CIP) network, a DeviceNet network, a ControlNet

network, an Ethernet network, DH/DH+ network, a Remote I/O network, a Fieldbus network, a Modbus network, or a Profibus network with the system disclosed in the mentioned references. Walker, Kabe, or Branstad do not disclose the use of a security field to limit access based upon line of sight parameters.

It is commonly known to one of ordinary skill in the art at the application date that communication protocols used within factory networks, such as TCP/IP or MAP, are comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field. It is also commonly known to one of ordinary skill in the art that various wireless, including those using line of sight parameters, and communication protocols can be used within an automated factory network, such as CIP, TKIP, EAP, Aziz/Diffie Protocol, Kerberos protocol, Beller-Yacobi Protocol, MSR+DH protocol, FPLMTS, Beller-Chang-Yacobi Protocol, Diffie-Hellman Key Exchange, Parks Protocol, ASPECT Protocol, TMN Protocol, RADIUS, GSM protocol, CDPD protocol. Furthermore, these various protocols can be used to establish the following networks: CIP, DeviceNet, ControlNet, Ethernet, DH/DH+, a Remote I/O, Fieldbus, Modbus, and Profibus. It is obvious to one skilled in the art that a method of providing network security, such as the one described in Walker, would be adaptable and implemented on multiple network protocols that existed at that time. It is also obvious to one skilled in the art that a method of providing network security can "tunnel" through multiple types of networks that use such network protocol, such as the ones described above. Furthermore, the use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network. The broad compatibility within networks and protocols available follows within the concept of allowing various components, which are more than likely to be manufactured by different vendors, to communicate seamlessly. Allowing access to the factory network wirelessly, virtually, or remotely improves the accessibility of the network and communications between an authorized user and component or between components.

4. Regarding Claims 22 and 23, Walker, in view of Kabe, and in further view of Branstad, discloses all the limitations of Claim 20 above. They do not specifically disclose that the security protocol comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field or that the path component further comprises of a requestor identifier.

It is commonly known to one of ordinary skill in the art at the application date that communication protocols used within factory networks, such as TCP/IP or MAP, are comprised of various combinations of a time component, message integrity component, digital signature, encryption field, sequence fields, pseudo random sequence, and dynamic security adjustment field. It is further known that within the communication protocol, information regarding both the sender and requestor of said information is embedded and used to facilitate the data transfer and to authenticate the sender and recipient. The use of the various combinations of the aforementioned components for any communication and security protocol ensures proper transmission and authorized access of information across a network.

Claims 25 - 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Kabe, in view of Branstad, and further in view of "AI Techniques Applied to High Performance Computing Intrusion Detection" by Susan M. Bridges et al. (hereinafter referenced as "Bridges").

8. Regarding Claims 25 - 31, Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data and provides path information for the data and comprises of a security and a performance parameter (pgs. 4 and 6, paragraphs 0035 and 0051). Walker, however, does not specifically use this method and apparatus within the automated factory setting or the utilization of an intrusion detection component or methodology. Walker also does not specifically disclose that the security system comprises of employing weak encryption protocols for real-time performance and strong security protocols for added security.

Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (col. 1, lines 14-24). The invention also discloses that within a factory automation environment, there is an international standard communication protocol called Manufacturing Automation Protocol (MAP) (col. 1, lines 15-18). The specific protocol used within the factory network is not what is relevant, but the disclosure that a communication protocol is used within the network to harmonize equipment used in the factory that are typically manufactured by different vendors (col. 1, lines 25-27). Kabe, however, does not specifically disclose that the security system comprises of employing weak encryption protocols for real-time performance and strong security protocols for added security. Furthermore, Kabe does not specifically disclose the utilization of an intrusion detection component or methodology.

Branstad discloses the use of various levels of security authentication mechanisms depending on various system conditions regarding security authentication speeds (Fig. 3; Col. 3, Lines 43-49, 54-56; Col. 4, Lines 2-7, 53-61). Branstad further discloses that the levels of security at one level may make network connections too slow to process real-time high-speed video (Col. 1, Lines 26-34) and that selectively authenticating data, as described above, is a method to remedy that issue. It would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Branstad with Walker and Kabe to modify the level of security authentication needed for the data packets being transmitted within the network. This would allow more urgent communications to be processed faster and decrease the time needed to authenticate data related to real-time media, such as streaming video and audio, which are intermittent if authentication mechanisms are too strong. Branstad, however, does not specifically disclose the utilization of an intrusion detection component or methodology.

Bridges discloses a system and method of using artificial intelligence within a high performance computer environment detect intrusions in the network. Specifically, Bridges discloses its use within a cluster computing architecture using both TCP/IP and Giganet networking protocols (pg. 1, paragraph 3). The system combines both anomaly and misuse detection mechanisms and uses both network traffic and system audit date as inputs, meaning the intrusion detection is both host and network-based (pg. 1, paragraph 1). Fuzzy logic is used with association rules and frequent episodes to "learn" normal patters of the system behavior. If certain events leave a set of patterns that are below a specified threshold, the system issues an alarm. The system can also implement rules that match patters of known attacks or patterns that are commonly associated with suspicious behavior to identify attacks (pg. 2, paragraph 5). The system also uses a Decision Module determine the security actions once an attack is detected (pg. 9, paragraph 1). It is obvious to one skilled in the art when the invention was made that an automation security system that will monitor for intrusions and unauthorized access is necessary due to the possibility of address spoofs or tunneling into the network. The Bridges system particularly functions well in an automated system where performance degradation is generally not acceptable. Furthermore, the ability of the Bridges system to use multiple communication protocols that are also usable in an automated security system makes the Bridges system very desirable as an intrusion detection system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. 2003/0014500; U.S. 5,539,906; U.S. 2003/0195861; U.S. 6,357,010; U.S. 6,477,651; U.S. 2002/0199122; U.S. 6,647,497; U.S. 2004/0073900;

U.S. 2003/0126466; U.S. 2002/0099959; U.S. 2002/0188870; "Manufacturing Automation Protocol (MAP): Review and Analysis," by Michael Kaminski, New Directions in M.I.S. Management: Seminar, Melbourne, FL, Nov. 13-15, 1985.

Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tae K. Kim, whose telephone number is (571) 270-1979. The examiner can normally be reached on Monday - Friday (8:00 AM - 5:00 PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton B. Burgess, can be reached on (571) 272-3949. The fax phone number for submitting all Official communications is (703) 872-9306. The fax phone number for submitting informal communications such as drafts, proposed amendments, etc., may be faxed directly to the examiner at (571) 270-2979.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

TKK

January 4, 2008

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/7/08